

Method and apparatus are disclosed including a system monitor which limits the ability of a program about to be executed to the use of predefined resources (e.g., data files, disk writing capabilities, etc.). The system monitor processes a data structure including a set of authorities defining that which a program is permitted to do and/or that which the program is precluded from doing. The set of authorities and/or restrictions assigned to a program to be executed are referred to as “program authorization information” (or “PAI”). Once defined, the program authorization information is thereafter associated with at least one program to be executed to thereby delineate the resources and functions that the program is allowed to utilize and/or is not allowed to utilize. The PAI associated with a particular program may be assigned by a computer system owner/user or by someone who the computer system owner/user implicitly trusts. The PAI permits an associated program to access what has been authorized and nothing else. The program may be regarded as being placed in a program capability limiting “safety box”. This “safety box” is thereafter associated with the program such that when the system monitor runs the program, the PAI for that program is likewise loaded and monitored. When the program is to perform a function or access a resource, the associated PAI is monitored to confirm that the operation is within the defined program limits. If [*sic*] the program is prevented from doing anything outside the authorized limits.

The following claims of the '591 Patent are relevant to claim construction (disputed terms emphasized):

1. In a computer system including *processing means for executing a plurality of programs* and memory means coupled to said *processing means* for storing data and for storing at least one program, said computer system having a plurality of computer resources and being capable of performing a wide range of information processing related functions under program control, a method for protecting a computer user from operations typically performable by a program while it is executing on behalf of a user, comprising the steps of:

establishing a *program authorizing information data structure* for storing a plurality of authorization entries each indicating at least one of those computer resources and information processing related functions which may be used by an associated program;

storing said *program authorizing information data structure*; and

associating the *program authorizing information data structure* with at least one program to be executed by said computer system to thereby protect the computer user from operations that might be performed by said at least one

program, whereby the program authorizing information is available to be monitored when its associated program is executed.

42. In a computer system having *means for executing a plurality of programs* and a memory means coupled to said means for executing, for storing data and program instructions, said computer system being capable of performing a wide range of information processing related operations under program control, a method for executing programs by said *means for executing* for a computer user comprising the steps of:

identifying a program to be executed;

determining whether a *program authorizing information data structure* has been associated with the program, wherein said program authorizing information qualifies the ability of the program from performing information processing related operations which are available to said computer user;

examining said *program authorizing information data structure* if one has been associated with said program;

determining from an examination of *said program authorization information* whether the associated program is allowed to perform an attempted information processing related operation; and

suppressing performance of said operation if said *program authorizing information data structure* indicates that said program is not allowed to perform an attempted operation.

The following claims of the '717 Patent are relevant to claim construction (disputed terms emphasized):

1. In a digital computer system having a digital data *processing means for executing a plurality of digital programs* and a memory means for storing digital program instructions and digital data, apparatus for protecting a digital computer user from operations typically performable by a digital computer program executing on behalf of a user comprising:

means for storing a plurality of *digital authorization entries* in said memory means, wherein said entries qualify operations which an associated program is permitted to perform when executed by said *processing means*; and

means for storing in at least one segment, digital data for associating said

authorization entries with at least one program.

10. Apparatus for protecting a digital computer user according to claim 1, wherein the means for storing a plurality of *authorization entries* includes means for indicating at least one of the type of function and resource said at least one program is permitted to perform for each of said entries.

61. In a digital computer system for providing improved computer security having digital data *processing means for executing a plurality of digital computer programs* for a computer user and memory means for storing digital program instructions and digital data, apparatus for protecting a digital computer user from operations typically performable by a digital computer program executing on behalf of a user comprising:

means for storing *digital authorization information* in said memory means which restricts an associated program from performing operations, when executed by said processing means, which are available to said computer user; and

means for storing in at least one segment digital data for associating said authorization information with at least one program to be executed by said *processing means*.

120. In a digital computer system having digital data *processing means for executing a plurality of digital computer programs* for a computer user and memory means for storing digital program instructions and digital data, a method for providing improved computer security comprising the steps of:

storing *digital authorization information* in said memory means which restricts an associated program from accessing resources when executed by said digital data *processing means* which are accessible to said computer user; and

storing in at least one segment, digital data for associating said authorization information with at least one program to be executed by said *processing means* for said computer user.

II. LEGAL PRINCIPLES

A determination of patent infringement involves two steps: first, the patent claims are construed, and, second, the claims are compared to the allegedly infringing device. *Cybor Corp. v. FAS Techs., Inc.*, 138 F.3d 1448, 1455 (Fed. Cir. 1998) (en banc). Claim construction is a

legal question for the courts. *Markman v. Westview Instruments, Inc.*, 517 U.S. 370, 391 (1996). The legal principles of claim construction were reexamined by the Federal Circuit in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). The Federal Circuit in *Phillips* expressly reaffirmed the principles of claim construction as set forth in *Markman v. Westview Instruments, Inc.*, 52 F.3d 967 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996), *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576 (Fed. Cir. 1996), and *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111 (Fed. Cir. 2004).

The Court construes the disputed terms in accordance with the doctrines of claim construction that it has outlined here along with those it has enunciated in the past. *See Pioneer Corp. v. Samsung SDI Co.*, No. 2:07-CV-170, 2008 WL 4831319, at *1-*5 (E.D. Tex. Mar. 10, 2008).

III. DISCUSSION

A. “[processing] means for executing a plurality of [digital] [computer] programs”

(1) The Parties’ Positions

This term applies to all of the above-quoted claims. The parties agree this is a means-plus-function term for “executing a plurality of programs” with the corresponding structure of “processor 2 and the equivalent structures thereof.” Dkt. Nos. 430 at 19 & 434 at 2. Defendant, however, proposes this term is indefinite. Dkt. No. 434 at 2.

Plaintiff argues this term is not indefinite because the operation of the processing means is well-known and is “irrelevant to the invention.” Dkt. No. 430 at 19. Plaintiff analogizes that if a patent claims a car alarm, the patentee need not disclose how a car’s engine works. *Id.* at 20.

Noting that the only corresponding structure is the general-purpose “processor . . . 2,”

Defendant relies on *WMS Gaming, Inc. v. International Game Technology*, 184 F.3d 1339 (Fed. Cir. 1999), to argue that the term “is indefinite because it is a means-plus-function element with only a general-purpose computer as its corresponding structure.” Dkt. No. 434 at 1 & 4; *see also* ’591 Patent at 4:51-52). Defendant further responds that Plaintiff’s car alarm analogy fails because the claimed invention is computer-related and because if a car alarm patent claimed a means for propulsion, the patentee would indeed be required to disclose some propulsive structure. Dkt. No. 434 at 5.

Plaintiff replies that “[t]he patents-in-suit describe apparatus and methods ‘for protecting’ the processing means,” “regardless of how they work.” Dkt. No. 435 at 2. Plaintiff argues that *WMS Gaming* is inapplicable because the means there was “called upon to perform unique, claimed functions,” whereas the “processing means” in the above-captioned case simply “operates to perform the basic function of all processors: executing programs — any programs.” *Id.* at 2-3.

(2) Construction

A determination of claim indefiniteness is a legal conclusion that is drawn from the court’s performance of its duty as the construer of patent claims. To the extent there are any factual findings upon which a trial court’s indefiniteness conclusion depends, they must be proven by the challenger by clear and convincing evidence.

Tech. Licensing Corp. v. Videotek, Inc., 545 F.3d 1316, 1338 (Fed. Cir. 2008) (citations and internal quotation marks omitted). A party asserting indefiniteness must overcome the statutory presumption of validity. *See* 35 U.S.C. § 282.

The recited “means for executing” is only relevant because other limitations interact with programs executed by the “means for executing.” In other words, the claims recite components

or operations that act upon the means, but the operation of the means does not bear on the scope of the claims. *WMS Gaming* and similar cases are therefore distinguishable. *See, e.g., Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech*, 521 F.3d 1328, 1333 (Fed. Cir.2008) (noting objective of avoiding “pure functional claiming”). On balance, the patentee’s failure to detail the operation of the “processor . . . 2” or the “means for executing” does not render the claims indefinite. *See Videotek*, 545 F.3d at 1339 (challenger failed to clearly and convincingly prove indefiniteness because details of structure at issue were well-known).

Defendants’ request that the claims at issue be found indefinite is therefore hereby DENIED.

B. Authorization-Related Terms

(1) The Parties’ Positions

The so-called “authorization related terms” are “program authorizing information data structure” (Claims 1 and 42 of the ’591 Patent), “digital authorization entries” (Claim 1 of the ’717 Patent), and “digital authorization information” (Claims 61 and 120 of the ’717 Patent). Dkt. No. 430 at 13. Plaintiff proposes constructions that include, in relevant part, “a set of authorizing and/or restricting segments.” Dkt. No. 430 at 13. Defendant would instead use the phrase “the set of authorities and/or restrictions assigned to a program to be executed.” Dkt. No. 434 at 6.

Plaintiff argues that the program authorizing information (“PAI”) need not be “assigned to a program to be executed,” as Defendant proposes, because “it may be generally defined to block *any* executing programs . . . access to certain resources and functions.” Dkt. No. 430 at 13. For example, Plaintiff submits that PAI can be “related to a user (not a certain program).” *Id.* at

14. Thus, Plaintiff argues, the PAI would not be assigned to a program but rather would merely be associated with a program upon execution. *Id.*

Defendant responds that “program authorization information” is explicitly defined in the specification as “the set of authorities and/or restrictions assigned to a program to be executed.” Dkt. No. 434 at 2. Defendant argues that Plaintiff’s proposal regarding segments is directed to an “exemplary” embodiment rather than the explicit definition. *Id.* at 6. Further, Defendant argues, other embodiments do not show the use of segments. *Id.* at 6-7.

In reply, Plaintiff reiterates the disclosure of authorizing and/or restricting segments and argues that Defendant’s proposal to include “assigned to a program to be executed” contradicts the specification, which discloses that the PAI “may” be assigned. Dkt. No. 435 at 4.

(2) Construction

The written description defines the following as “program authorization information (or ‘PAI’): “the set of authorities and/or restrictions assigned to a program to be executed.” ’591 Patent at 2:21-23.

First, the specification illustrates and describes “an exemplary program authorization information (PAI) data structure” that has “segments,” but Plaintiff has not shown that such disclosures are anything other than “exemplary.” *See* ’519 Patent at 5:3-4. Plaintiff submitted during oral argument that the “segments” are necessary for the claimed inventions to be operable. *See* Dkt. No. 446 at 14:9-10. But the canon that claims be construed to uphold their validity is only a guideline to be applied “if possible.” *Rhine v. Casio, Inc.*, 183 F.3d 1342, 1345 (Fed. Cir. 1999). At least as important is the canon that limitations not be imported from the specification. *Phillips*, 415 F.3d at 1323 (noting “danger of reading limitations from the specification into the

claim”); *see also* *Arlington Indus., Inc. v. Bridgeport Fittings, Inc.*, --- F.3d ----, 2011 WL 179768, at *5-*7 (Fed. Cir. Jan. 20, 2011) (reversing importation of limitation from specification). On balance, Plaintiff’s proposal to include “segments” in the construction would improperly import a limitation from a preferred embodiment and is therefore rejected.

Next, although the intrinsic definition of “PAI” leaves open the possibility that the term “PAI” could be used with programs other than “a program to be executed,” the above-quoted claims of the ’591 Patent themselves recite “associating” the PAI with a program “to be executed.” For example, Claim 1 of the ’591 Patent recites, in relevant part: “associating the program authorizing information data structure with at least one program to be executed by said computer system.” The above-quoted claims of the ’717 Patent recite authorization information or entries that have been “associated” with a program and that set forth how a program is permitted to perform “when executed.” Because the claims themselves should be considered first and foremost in construing claim terms, this explicit claim language governs. *See Phillips*, 415 F.3d at 1312, 1314.

Finally, Plaintiff submits that a PAI could be associated with a user rather than a program. *See* Dkt. No. 430 at 14. The written description does describe systems with multiple users:

FIG. 3D exemplifies a situation in which many users access the same program (image)--each having their own (possibly distinct) Program Authorization Information 129 associated with it and maintained in a specific file belonging to the user. . . . Thus, different users may limit a program according to their own needs and perception of trust.

. . .

[U]sers could define general PAI “association”, so that a protecting PAI could be automatically associated with all programs

’519 Patent at 8:45-9:2. Nonetheless, even this disclosure frames PAIs as being associated with

particular programs, even if a program may be the subject of multiple PAIs, such as for multiple users. On balance, none of the disclosure cited by Plaintiff justifies departing from the plain reading of the claims, as set forth above. The constructions of the disputed terms should therefore include the following language proposed by Defendants: “assigned to a program to be executed.”

The Court hereby construes “**program authorizing information data structure**” to mean “**a data structure for program information that includes the set of authorities and/or restrictions assigned to a program to be executed.**”

The Court hereby construes “**digital authorization entries**” to mean “**the set of authorities and/or restrictions assigned to a program to be executed.**”

The Court hereby construes “**digital authorization information**” to mean “**digital information that includes a set of authorities and/or restrictions assigned to a program to be executed.**”

C. Remaining Terms

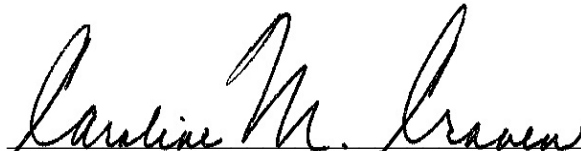
The Court need not address the remaining terms, on which the parties have agreed.

IV. CONCLUSION

The Court hereby **ORDERS** the disputed claim terms construed as set forth above.

IT IS SO ORDERED.

SIGNED this 7th day of February, 2011.


CAROLINE M. CRAVEN
UNITED STATES MAGISTRATE JUDGE